WE CLAIM:

1. A method of generating a cryptosync for a communication session between two communication devices, comprising:

deriving a value of a first cryptosync for the communication session based on a value of a second cryptosync, the second cryptosync having a longer life than the first cryptosync.

2. The method of claim 1, wherein the second cryptosync is used for message encryption by at least one of the two devices.

3. The method of claim 2, wherein the second cryptosync is used for verifying message integrity by at least one of the two devices.

4. The method of claim 1, wherein the second cryptosync is used for verifying message integrity by at least one of the two devices.

5. The method of claim 1, wherein the second cryptosync changes between communication sessions.

6. The method of claim 1, wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync.

7. The method of claim 6, wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence.

8. The method of claim 7, wherein the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence.

9. The method of claim 8, wherein the fixed bit sequence is a string of 0s.

10. The method of claim 8, wherein the deriving step derives a 32 most significant bits of the first cryptosync as the second cryptosync and derives a 32 least significant bits of the first cryptosync as a string of 0s.

11. The method of claim 6, wherein the deriving step derives a portion of the first cryptosync as the second cryptosync.

12. The method of claim 11, wherein the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence.

13. The method of claim 12, wherein the fixed bit sequence is a string of 0s.

14. The method of claim 1, wherein the deriving step comprises:

performing a pseudo-random function on the second cryptosync; and

generating the first cryptosync from output of the pseudo-random function.

15. The method of claim 14, wherein the generating step generates the first cryptosync as the output of the pseudo-random function.

16. The method of claim 1, wherein the deriving step is performed at a base station.

17. The method of claim 1, wherein the deriving step is performed at a mobile station.

18. The method of claim 1, further comprising:

encrypting a frame of information to send from the at least one of the two devices using the first cryptosync.

19. The method of claim 18, wherein the frame of information is a radio link protocol, RLP, frame.

20. The method of claim 18, further comprising:

incrementing the first cryptosync after the encrypting step.

21. The method of claim 1, further comprising:

decrypting a frame of information received at the at least one of the two devices using the first cryptosync.

22. The method of claim 21, wherein the frame of information is a radio link protocol, RLP, frame.

23. The method of claim 21, further comprising:

incrementing the first cryptosync after the decrypting step.

24. A method of generating a cryptosync for a communication session between two communication devices, comprising:

deriving a value of a first cryptosync for the communication session based on a value of a second cryptosync used to encrypt further communication between the two devices.